Monthly Security Tips NEWSLETTER

Department of Accounting and General Services
Information & Communications Services Division

July 2010 **Volume 5, Issue 7**

Protecting Data Contained in Copiers and Printers

What kind of data can be stored in copiers and printers?

You are probably familiar with many of the standard best practices for safeguarding your data, such as avoid carrying unencrypted sensitive data on portable devices; use a complex password; and keeping your PC current with updated anti-virus software and security patches. However, do you realize that another important aspect of safeguarding your data means taking precautions about the information contained on printers or copiers?

Increasingly, printers, copiers and related devices come with hard drives capable of storing large volumes of information. The data you print, copy, scan, or fax may be stored on the hard drive permanently.

Recent news coverage has highlighted the fact that confidential information can be recovered from printers, copiers and similar devices after they are sent to surplus or returned to the vendor at the end of their lease. Some of the confidential information recently reported to be found on these machines included social security numbers, birth certificates, bank records, income tax forms, medical records, and pay stubs with names.

How do I keep my data secure?

Assume that any document that you printed or scanned is stored on the device. At a minimum, be aware that when you dispose of your printer, fax, copier or scanner, there may be a hard drive containing images of all of your documents. In order to properly dispose of the device, have the hard drive securely wiped before you give the device away or sell it, or if the device's hard drive is removable, remove the drive entirely and have it securely destroyed.

Individuals and organizations should review the following recommendations for printers, copiers, scanners, and faxes:

- **Settings**: Configure the devices to encrypt the data, if possible.
- **New Devices**: Purchase\lease devices with disk encryption and immediate data overwriting capability.
- **Disposal**: Remove or wipe the hard drive before disposal.
- **Use of Public Devices**: Be cautious if using public printers\copiers\scanner\faxes for documents containing confidential information.

Additional Information:

- Identity Theft Awareness: http://www.identity-theft-awareness.com/digital-copiers.html
- Identity Theft Fixes: http://www.identitytheftfixes.com/company_copiers_and_identity_theft_--_is_your_company_at_ris.html
- CBS News - Digital Photocopiers Loaded With Secrets: http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml
- SANS Reading Room: http://www.sans.org/reading_room/whitepapers/networkdevs/auditing-securing-multifunction-devices_1921
- Xerox: http://www.xerox.com/information-security/product/enus.html
- Cannon: http://www.usa.canon.com/cusa/production/standard_display/security-main-page
- HP: http://h71028.www7.hp.com/enterprise/cache/617575-0-0-225-121.html
- Toshiba: http://www.copiers.toshiba.com/usa/security/device-security/index.html

For more monthly cyber security newsletter tips visit: www.msisac.org/awareness/news/

Brought to you by:

Information & Communications Services Division (ICSD) **Cyber Security Team** www.cybersecurity.hawaii.gov The mission of the ICSD **Cyber Security Team** is to preserve the confidentiality, integrity, and availability of the State of Hawaii's electronic information resources.	Multi-State Information Sharing & Analysis Center www.msisac.org The mission of **MS-ISAC** is to provide a common mechanism for raising cyber security readiness and response in each state and with local government.

The information provided in the Monthly Security Tips Newsletters is intended to increase your security awareness and to help improve the organization's overall cyber security posture.